Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In re:	)	
	)	
Digital Broadcast Copy Protection	)	MB Docket No. 02-230

REPLY COMMENTS OF THE NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION

The National Cable & Telecommunications Association ("NCTA") hereby submits its reply comments in the above-captioned proceeding. As we observed in our initial comments, NCTA supports the Commission's efforts to facilitate digital broadcast copy protection. In particular, we support efforts to implement the "broadcast flag" with the limited purpose of preventing re-distribution of high value digital content over the Internet as described in the Notice of Proposed Rulemaking ("Notice") adopted in this proceeding. However, implementation of the broadcast flag must provide for sufficient flexibility so that cable – and other media – may satisfy the purpose underlying the broadcast flag by means tailored to those different media which are most conducive to those media and the customers they serve.

As we noted in our initial comments, representatives of NCTA and other cable interests actively participated in the Broadcast Protection Discussion Group ("BPDG") discussions and the development of its proposal that over-the-air television receivers should read and respect embedded digital instructions in digital television ("DTV") broadcasts that instruct the devices not to engage in unauthorized redistribution of digital broadcast programming over the Internet. While cable interests – like others – remain concerned about some provisions in the "final" BPDG Report as submitted in the record in this proceeding, we supported the concept of a

broadcast flag with the limited purpose of restricting appropriately-marked digital broadcasts against Internet retransmission, as proposed in the Notice.

Nevertheless, our initial comments raised a number of concerns – about process and substance – that have only been reinforced by other comments filed in this proceeding. As a threshold matter, our comments stressed that any broadcast flag or similar technology be limited in purpose and scope. That is, its sole purpose should be to prevent the unauthorized re-distribution of high value digital broadcast content over the Internet. In this regard, we said that the Commission should assure that the proposed three bytes comprising the Redistribution Control descriptor be limited to a simple on or off function, used solely to signal consumers' over-the-air television receivers not to engage in unauthorized redistribution of digital broadcast programming over the Internet, and not for other purposes.

Our initial comments also emphasized that the Commission should not adopt a "one size fits all" approach to implementation of a broadcast flag since different media can protect against Internet retransmission of digital broadcast signals through different techniques that achieve the same functional result. In particular, we noted that it is not necessary to embed the Redistribution Control descriptor when a broadcast signal is managed at the cable headend, so long as the appropriate instruction is delivered to a digital television receiver or other device connected to the cable system.

Such a flexible approach is necessary so that consumers may receive the benefits of home networking, delivered by cable systems or others. Maintaining the flexibility to develop a secure home network will allow greater dissemination of programming within the home for private home use. We also urged that any FCC rules should accommodate the ability to innovate and rapidly deploy new secure outputs and interfaces, without compromising existing secure

consumer choice technology solutions. In this regard we noted that the selection and expansion of authorized digital output protection technologies and authorized recording methods (the "Table A" issue) should be the result of a timely, fair, reasonable and nondiscriminatory process using a combination of both "market-based" criteria and technical criteria. The rules should also be sufficiently flexible so that publishers and distribution media may promptly respond to consumer reaction, hacking, and similar market changes.

Scope Limitations: Our initial comments explained that the purpose of the broadcast flag should be limited to restrictions against unauthorized redistribution of digital broadcast content over the Internet. While the thousands of comments filed in this proceeding differ on whether the broadcast flag (whether implemented by the FCC, by industry consensus or otherwise) is the correct solution to the concern about unauthorized distribution over the Internet, it is generally recognized that such unauthorized Internet redistribution is a serious concern. But, in the BPDG discussions, as well as in this proceeding, concerns have been expressed that some may want to expand the functionality of the flag to implement copy control mechanisms, or to restrict traffic on other networks, including home networks.

The flag must be limited to its original purpose. It should not be turned into a vehicle for restricting home use within a secure home network, or for carrying other transactions or instructions. The broadcast flag should be limited to its intended use, and not be made unnecessarily complex or be put to a use for which there is no consensus – not even among the BPDG in its Final report. As proposed in the Notice, the scope of the proposed broadcast flag solution should be limited to what is intended and needed to protect content providers' interests against unauthorized Internet retransmission of their high value content. As we said in our initial comments, the proposed broadcast flag, the Redistribution Control descriptor, consists of three

bytes (24 bits) of data, including eight bits for "optional additional information that may be defined in the future."[1] This is more capacity than is required to instruct the receiver to protect against unauthorized redistribution over the Internet. In order to avoid unintended uses (or abuses) of such a dataflow, which flows directly to subscriber equipment, the Commission should include a limitation on any extraneous uses of the broadcast flag. The proposed Redistribution Control descriptor should be confined to the specific 24 bit value needed for that purpose, and its use should be limited to that specific function.

Professional Equipment Exemption: Part of the flexibility that we believe must be accorded the cable industry in implementing a broadcast flag solution is the industry's ability to manage a broadcast signal at the cable headend in the most efficient manner possible so long as the appropriate instruction is delivered to a digital television receiver connected to the cable system. Likewise, cable operators may choose to protect content through various security arrangements. For example, analog HBO transmissions are routinely scrambled because of the ubiquity of analog tuners. Digital broadcast channels may likewise need to be encrypted to protect against unauthorized reception by QAM tuners.

In this regard, as noted in our comments, participants in the BPDG discussions agreed that there should be a professional equipment exemption to any broadcast flag rules, but the Final BPDG Report did not include such an exemption.[2] There appears to be no disagreement among commenters on this point. Accordingly, the Commission, in any rules it adopts in this area, should provide a "professional equipment" exemption so that operations at the cable

---

[1] Amendment No. 3 to Revision A of ATSC Standard: Program and System Information Protocol for Terrestrial Broadcast and Cable, Doc. A/65A – (31 May 2000), Doc. T3-556, April 1, 2002.

[2] BPDG Report Tabs D and E – alternative X.2 riders prepared by certain MPAA and CE/IT BPDG representatives, at footnote 1 ("We *anticipate* that an appropriate provision would be crafted so as to exempt

headend are permitted to operate routinely, protecting content even if they do not follow the rules applied to an end-user consumer.

Secure Home Networks: In our comments we stressed the importance of preserving cable's flexibility to implement home networking solutions for consumers without being limited (unintentionally or not) by restrictions surrounding distribution within the home of material containing the broadcast flag. As we said, cable operators are increasingly involved in managing secure home networks for consumers who wish to share modems, printers and home gateways, and who wish to move programming around the secure home network for private home use. As these secure home networks emerge, consumer and market-driven security measures that are different from – but equally effective as – the proposed broadcast flag may be employed within the secure home network.

Just as content may be securely managed at the headend and transported over cable systems using a variety of protection technologies, the same flexibility should be extended through a secure home network. As originally submitted by the co-chairs, the BPDG Report had preserved this crucial developing market of secure home networks. It had left open the possibility that Marked Content – that is, broadcast programming marked to restrict against Internet redistribution – could be output using "robust methods." This meant that a cable operator, for example, could use various forms of encryption, conditional access, and other security tools to carry Marked Content from one set-top box (for example, in the living room) to another (for example, in the bedroom), so long as the home network itself used secure interfaces between set-top boxes, so that Marked Content would not leak onto the Internet.

---

these requirements from applying to products that are specifically intended for professional video and broadcast use.") (emphasis added).

Some comments have suggested changes in the BPDG Report that would eliminate the option to output Marked Content over robust outputs, and instead require that home networks pass all broadcast signals (or at least all broadcast signals including Marked Content) as unaltered unscreened content.[3] A change of this nature would seriously impede the operation of secure home networks. A receiver ("demodulator") connected to a home network typically "alters" the demodulated stream by de-multiplexing it to separate out a desired broadcast television program from other programs or data in the digital channel. This "altered" content on a secure home network is only the desired MPEG program, not the entire MPEG transport stream. It is not at greater risk of theft, but can be carried at far more efficient bit rates over the network. A VHS quality program can be carried at about 1 Mbps; a standard definition program can be carried at perhaps 4 Mbps, and a HDTV program can be carried at 12 Mbps. By contrast, for carriage on a secure cable home network, the entire unaltered MPEG transport stream delivered by a cable standard 64-QAM or 256-QAM demodulator would require 27 Mbps (at 64 QAM) or 38.8 Mbps (at 256 QAM).

If the only option for a secure home network is to carry unaltered streams from the demodulator, then content that could have been carried over a secure home network at 1, 4, or 12 Mbps would now need to be carried at 27 or 38.8 Mbps. Many home networks struggle to deliver two or more programs at the 1 to 5 Mbps rates that are common for standard definition television. Requiring carriage of digital broadcast content at the data rates required for full unscreened unaltered signals would impose significant overloads in transport around the home, lock-up of home devices, and failure of home networks when broadcast signals are carried. (By

---

[3] See Joint Comments of the Motion Picture Association of America, et. al., at Attachment A, Section 5.4 ("MPAA Comments").

contrast, there would be no equivalent overloads or lock-ups for cable programs, which are outside of the scope of the flag.)

It is far better, and far more conducive to the development of home networks, to permit Marked Content to be carried as "altered," screened for the flag, and de-multiplexed throughout a secure home network. Within the secure home network, Marked Content would be protected using whatever carrier and protocol the operator chooses to protect the security of the network. When the content leaves the secure home network, for example, if it is output through a 1394/5C port on a set-top box, it would be marked (flagged) for protection against Internet retransmission, presumably by setting the 5C EPN bit at the 1394 interface. Marked Content would therefore be protected within the secure home network, and protected when it leaves that network. Therefore, in implementing any broadcast flag solution, the Commission should maintain cable's flexibility to develop secure home network approaches that will allow for the maximum distribution of programming within the home for private use.

Authorized Outputs/Technologies ("Table A"): As we noted in our initial comments, participants in the BPDG discussions were also divided over how "outputs" are to be "authorized." No one disputed the need to assure that any new interface fully support applicable content protection, but no consensus was reached on how to balance the ability to innovate and rapidly deploy new interfaces with the need to make certain any such new interfaces were truly secure. These issues deal with the "approved" outputs listed on "Table A."

In our comments we emphasized that, whatever process is selected for adding authorized outputs to Table A, it must be clearly defined, rapid, inclusive of all parties, and include definite timetables for approval and appeal procedures before a neutral decision-making body. Because business models and technology solutions in video distribution and home networking move at a

fast pace, likewise, the process for approval of technologies must move quickly. Therefore, we suggested that a combination of both "market-based" criteria (such as the proposal set forth at Tab F of the BPDG Report) and technical criteria (such as the proposal set forth at Tab G of the BPDG Report) would be the most effective approach.

While the debate over the proper criteria for Table A authorization has now moved from the BPDG discussion context to the FCC comment process, there continues to be no consensus on appropriate criteria for including outputs in Table A. NCTA is particularly concerned about comments that suggest that, under some circumstances, new connectors may have to pass through an FCC process that also evaluated the intellectual property license terms and price of proprietary technologies used in new interfaces.[4]

The concerns arising from such an approach are particularly acute if Table A were to limit outputs in a secure home network system. As identified in ITU recommendations and CableLabs specifications, there are already a wide variety of wireless and wired home networks.[5] Already there are disquieting signs in the broadcast flag comments that if certain criteria are required for inclusion of outputs in Table A's "authorized list," that might disadvantage or delay many of these home network technologies.

For example, Table A would allow internal interfaces across a PCI bus (the user accessible part of a computer designed to accommodate the addition of various drives and ports). However, there is no quick, efficient and inexpensive path for the prompt addition of competing

---

4 MPAA Comments at 23 and Attachment C.

5 Physical Media include Coaxial Cable, CAT 5 and CAT 6 cable, telephone wire, power lines, optical fiber, RF wireless, Infrared wireless. Protocols include Bluetooth™, Ethernet (IEEE 802.3), HomePlug™, HomePNA™, HomeRF™, IEEE 802.11a and 802.11b wireless. New networking methods will very likely be added to these lists as consumer preferences and the technology limitations of current methods become clear.

technologies to Table A when designing secure home networks that do not utilize the PCI bus.[6] Without far better criteria for evaluating additions to Table A, with definite timetables for approval and appeal procedures before a neutral decision-making body, Table A may become a barrier to innovation. It is particularly ill-suited to govern what should be a rapid evolution of competing secure home network technologies.

CONCLUSION

[6] As an analogy, 1024 QAM is already in Broadcom chips, but the proposed regulations suggest that only 64 and

For the reasons stated above and in our initial comments, NCTA supports Commission implementation of a broadcast flag for the limited purpose of protecting against the unauthorized re-distribution of high value digital broadcast content over the Internet. However, the rules implementing the broadcast flag requirement must provide for flexibility so that different media may protect against Internet retransmission of digital broadcast signals in the manner best conducive to that media through techniques that achieve the same functional result. In particular, there should be exemptions for cable professional equipment (e.g. headend equipment) and rules that recognize the importance of permitting flexibility for cable and others to develop secure home networks and home networking solutions that will allow consumers the maximum ability to distribute programming within their homes for private use. Finally, there must be a timely, fair, reasonable, and non-discriminatory process for adding (or deleting) outputs and technologies from Table A's approved outputs list.

Respectfully submitted,

/s/ Daniel L. Brenner

Daniel L. Brenner
Neal M. Goldberg
National Cable & Telecommunications Association
1724 Massachusetts Avenue, N.W.
Washington, D.C. 20036-1903
(202) 775-3664

Paul Glist
Cole, Raywid & Braverman, L.L.P.
1919 Pennsylvania Avenue, N.W.
Suite 200
Washington, D.C. 20006
(202) 659-9750

February 20, 2003

256 QAM are permitted. This is the type of regulatory lag that should be avoided.